IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF: EVIDENCE CURRENTLY LOCATED AT: HOMELAND SECURITY INVESTIGATIONS 3000 SIDNEY STREET, SUITE 300 PITTSBURGH, PA 15203, WHICH IS PARTICULARLY DESCRIBED IN ATTACHMENT A	Magistrate No. 3:21-162 MJ

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Jason Adams, a Special Agent (SA) with Homeland Security Investigations, being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property – three electronic devices (herein after referred to as "**TARGET DEVICES**"), as described in Attachment A - which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Department of Homeland Security ("DHS"), Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI"), currently assigned to the Pittsburgh, Pennsylvania office. I have been so employed since July 2009. As part of my duties as an HSI Special Agent, I investigate criminal violations relating to high technology crime, cyber-crime, child exploitation and child pornography including violations pertaining to the illegal distribution, receipt, possession, and production of materials depicting the

sexual exploitation of children in violation of Title 18, United States Code, Sections 2252 and 2251. I have received training in the area of child pornography and child exploitation investigations, and I have had the opportunity to observe and review numerous examples of such materials in a variety of electronic media. I am a member of the Western Pennsylvania Internet Crimes Against Children ("ICAC") Task Force. I have participated in and led numerous child pornography investigations. I have executed numerous search warrants related to child pornography investigations. In this regard, I have reviewed extensive samples of child pornography, including videos, photographs, and digital reproductions of photographs or other print media.

3. The statements contained in this affidavit are based upon my investigation, information provided by other sworn law enforcement officers and witnesses, other personnel specially trained in the seizure and analysis of computers and electronic mobile devices and electronic storage devices, and on my experience and training as a federal agent.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on the information set forth in this affidavit, there is probable cause to believe that on the **TARGET DEVICES** there exist fruits, instrumentalities, contraband, and evidence of violations of Title 18, United States Code, Section 2252(a), which makes it a crime to receive, distribute, and possess material depicting the sexual exploitation of a minor (child pornography). I am requesting authority to search the entirety of the **TARGET DEVICES**, for the items specified in Attachment B, hereto, which items constitute fruits, instrumentalities, contraband, and evidence of the foregoing violations.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

6. The property to be searched (hereinafter "**TARGET DEVICES**") is described as follows:

a. Motorola Mobile Telephone, Blue in Color

b. Thumb Drive, Red and Silver in Color

c. Digital Voice Recorder, Gray in Color

7. The **TARGET DEVICES** are currently located at HSI Pittsburgh, 3000 Sidney Street, Suite 300, Pittsburgh, PA 15203.

8. The applied-for warrant would authorize the forensic examination of the **TARGET DEVICES** for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

9. On July 20, 2021, your affiant was connected to the BitTorrent P2P network conducting investigations into the sharing of child pornography over the Internet. The investigation was focused to a device at IP address 137.103.160.62 because it was associated with a torrent with the infohash: 983904bc3b32f025f384048085c0de7618bcb8bf. This torrent file references a file identified as being a file of investigative interest to child pornography investigations. Using a law enforcement computer located at the Homeland Security Investigations office in Pittsburgh, Pennsylvania running investigative BitTorrent software, a connection was made to the device at IP address 137.103.160.62, hereinafter referred to as "Suspect Device". The Suspect Device reported it was using BitTorrent client software Transmission 2.94. On or about July 20, 2021, from 1651 hours and 1751 hours (UTC -

4:00:00), your affiant downloaded approximately three files and partially downloaded approximately six files, that the Suspect Device was making available. The Suspect Device at IP Address 137.103.160.62 was the sole candidate for the download, and as such, the file was downloaded directly from this IP Address. Your affiant has reviewed the downloaded files and observed multiple videos that depict prepubescent minor females engaged in sexually explicit conduct. Your affiant describes one of these files as follows:

a. A video with file name 000005.avi that is approximately five minutes and 43 seconds in length depicts a prepubescent minor female with brown hair, estimated to be 8 to 10 years of age, performing oral sex on an adult male visible from stomach to feet. The video then shows a second prepubescent minor female estimated to be 6-8 years of age and a third minor female estimated to be 8 to 10 years of age, and both minor female's breasts and vagina are exposed to the camera. The video then shows the first minor female again lying on her back with breasts and vagina exposed as the camera zooms in and shows an adult male's hand touching her vagina.

10. On August 24, 2021, your affiant was connected to the BitTorrent P2P network conducting investigations into the sharing of child pornography over the Internet. The investigation was focused to a device at IP address 137.103.160.62 because it was associated with a torrent with the infohash: 610b27f1d2639e9d697aecc56d05a8510d6f7550. This torrent file references a file identified as being a file of investigative interest to child pornography investigations. Using a law enforcement computer located at the Homeland Security Investigations office in Pittsburgh, Pennsylvania running investigative BitTorrent software, a connection was made to the device at IP address 137.103.160.62, hereinafter referred to as "Suspect Device". The Suspect Device reported it was using BitTorrent client software -TR2940- Transmission 2.94. On or about August 24, 2021, from 0359 hours and 0553 hours (UTC -4:00:00), your affiant downloaded approximately 83 files that the Suspect Device was making

available. The Suspect Device at IP Address 137.103.160.62 was the sole candidate for the download, and as such, the file was downloaded directly from this IP Address. Your affiant has reviewed the downloaded files and observed multiple videos that depict prepubescent minor females engaged in sexually explicit conduct. Your affiant describes one of these files as follows:

a. A video with file name 000284.avi that is approximately one minute and one second in length depicts multiple segments of a prepubescent minor female with brown hair wearing dark sunglasses, estimated to be 8 to 10 years of age. The first segment shows the minor female nude, standing in a shower with her arms behind her head, facing the camera with her breasts and vagina predominately displayed. The next segment shows same minor female lying on her back on a bed with white pillows and blue and white sheets, while a partially viewable adult male attempts to insert his penis into her vagina. The next segment shows the minor female seated on top of the nude adult male on a bed and having sexual intercourse. The next segment shows the minor female masturbating the adult male. The last segment shows the minor female fully dressed in a blue t-shirt, blue pants, and blue headband, standing next to the bed.

11. A check of publicly available records located online by an organization known as the American Registry of Internet Numbers, determined that the IP address 137.103.160.62 was assigned to a company known as Atlantic Broadband on July 20, 2021. On or about July 28, 2021, a federal summons to identify the IP Address history of the subscriber of IP address 137.103.160.62 was served to Atlantic Broadband. On or about July 28, 2021, a response to the summons identified that on July 20, 2021, from 1651 hours and 1751 hours (UTC -4:00:00), and August 24, 2021, from 0359 hours and 0553 hours (UTC -4:00:00), the subscriber was JOSEPH and LUCIEN SCOTT with the address **1008 21ST AVE., ALTOONA, PA 16601**.

12. On or about July 28, 2021, your affiant conducted a check in Pennsylvania Department of Transportation records which revealed identification number 34004779 had been issued to LUCIEN MALLORY SCOTT with the date of birth March 30, 2001. The address listed

on this identification is 1008 21ST AVE., ALTOONA, PA 16601.

13. On or about August 13, 2021, your affiant conducted a record check with the Pennsylvania Office of the Inspector General which revealed that in May of 2021, JOSEPH and LUCIEN SCOTT had reported the address 1008 21ST AVE., ALTOONA, PA 16601 in relation to an application for state benefits. The date of birth on this record for JOSEPH SCOTT is April 17, 1978. The date of birth on this record for LUCIEN SCOTT is March 30, 2001.

14. On or about August 30, 2021, your affiant conducted surveillance at 1008 21ST AVE., ALTOONA, PA 16601. During this surveillance, your affiant observed and obtained photographs of the residence. Your affiant can describe this residence as a three (3) story, single family residence, primarily of red brick construction with enclosed porch with white siding, gray roof, and entrance located at 21st Avenue. The numbers "1008" are displayed in black text on the white siding near the entrance door.

15. On October 13, 2021, your affiant made application for and was issued a federal search warrant by United States District Court, Western District of Pennsylvania for the residence located at 1008 21ST AVE., ALTOONA, PA 16601. This search warrant was executed on October 19, 2021. During the search warrant, JOSEPH DAVID SCOTT (SCOTT) was encountered at the residence and he agreed to a consensual interview with your affiant. During this interview, SCOTT confirmed that his computer is a custom computer located in the bedroom at the top floor of the residence. SCOTT stated that he had previously viewed child porngraphy on the internet but had reported it to the FBI. SCOTT also admitted that he used BitTorrent peer-to-peer, file-sharing client program called "Transmission" and this software program is currently installed on his customer computer. The program "Transmission" is associated with the two distribution dates of

child pornography in this investigation, as described in paragraphs 6 and 7. Your affiant asked SCOTT which computers child pornograpy would be present on and he stated that his oldest minor son uses the "Transmission" program on his computer but it wouldn't make sense for it to be his son.

16. On October 21, 2021, HSI Computer Forensics Agent David Coleman (CFA Coleman) conducted further forensic review of SCOTT'S custom computer and observed approximately 291 named video files in the folder: root/seidleitr/Videos/Erotica/Frostwire that occupy approximately 56.1GB of disk space. CFA Coleman advised your affiant that most of these video files have titles that are assocated with child pornography and CSAM materials including but not limited to "pthc", "ptsc", "hussyfan", "R@ygold", "children", "preteen", and "pedo". CFA Coleman describes the following relevant sampling of these videos as follows:

a. A video with file name "!!! NEW !!! 2010 kait 5yo - chunk2 FK pthc best.avi" is a video file that is 76.0MB in file size and 1 minutes, 25 seconds in duration. This video depicts a prepubescent female child approximately 4 to 6 years in age being vaginally penetrated by an adult male penis.

b. A video with file name "(Pedo) Pedoland - 5Yo And 12Yo 07 Childporn 7Yo Suck Man (Pthc Babyj Pedo)Extended Version.avi" is a montage video file that is 89.8MB in file size and 15 minutes, 4 seconds in duration. This video depicts a prepubescent female child approximately 6 to 8 years in age being vaginally penetrated by an adult male penis and performing oral sex on an adult male penis.

c. A video with file name "pthc_2010_toddlergirl_kait_5yo_golden_shower_on_dad_wmv.mpg" is a video file that is 69.2MB in file size and 5 minutes, 23 seconds in duration. This video file depicts a minor female child approximately 4 to 6 years in age performing oral sex on an adult male penis, manually masturbating an adult male penis, and being directed to urinate on the adult male.

17. On October 21, 2021, your affiant made application for and was issued a federal arrest warrant by United States District Court, Western District of Pennsylvania for SCOTT in

relation to violations of Title 18, United States Code, Sections 2252(a)(4)(B) as it relates to possession of materials depicting the sexual exploitation of a minor. This same day, your affiant, and Agents and Officers with the Pennsylvania Attorney General's Office, Johnstown Police Department, and the Altoona Police Department attempted to locate and arrest SCOTT at his last known residence of 1008 21st Ave., Altoona, PA 16601. However, SCOTT was not located.

18. On October 21, 2021, your affiant was informed by Altoona Police Department that SCOTT attempted to purchase a firearm at Northern Supply Guns and Ammo located at 1006 North 4th Avenue, Altoona, Blair County, PA. An employee of this firearms store subsequently informed your affiant that SCOTT had attempted to purchase an AK-47 rifle, an AR-15 rifle, and two (2) firearms. The employee stated that SCOTT was denied purchasing the firearms due to having an out-of-state driver's license from the state of Arizona.

19. On October 23, 2021, your affiant was informed that the HSI Special Agent Robert Connelly (SA Connelly) and the Richland Police Department located in Johnstown, PA, Cambria County, encountered a vehicle near the Richland Towne Center, Johnstown, PA, registered to Danielle Biconik, the girlfriend of SCOTT. The vehicle, a 2012 Nissan bearing PA license plate number HXN-2054, was located and found to be occupied by Lucien Scott, SCOTT'S son, and Danielle Biconik after SA Connelly observed Lucien Scott returning from Wal-Mart with a tent, sleeping bag and boots. Richland Township Police Officer Zada asked the location of SCOTT and Lucien Scott stated his father walked away from the Econolodge, located in downtown Johnstown, and has not seen him since.

20. On October 24, 2021, your affiant spoke with Lucien Scott, son of SCOTT, via telephone, and he stated he and his father had left the residence of 1008 21st Avenue, Altoona,

PA, Blair County and were staying at a hotel in Altoona, PA, because law enforcement had been visiting their residence at 1008 21st Avenue, Altoona, PA 16601.

21. On October 25, 2021, your affiant was informed that this same day at approximately 0119 hours, Johnstown Police were dispatched to Sheetz, 208 Haynes Street, Johnstown, Cambria County for Joseph SCOTT. Johnstown Police arrived on scene and located SCOTT. SCOTT was taken into custody without issue. While being processed, SCOTT stated he had been staying on the hillside above the Dollar General Store in downtown Johnstown. Johnstown Police transported SCOTT to the Cambria County Prison. At the time of his arrest and his placement in custody of the Cambria County Prison, SCOTT was wearing clothing consisting of mainly pants, shoes, socks, shirt and/or sweatshirt/jacket. Also, at the time he was placed in custody of the Cambria County Prison, SCOTT was in possession of a backpack containing, among other items, handcuffs, and the **TARGET DEVICES**.

22. On October 25, 2021, your affiant was informed by Johnstown Police Department Detective Mark Britton (Det. Britton) that he had obtained a state search warrant to take custody of SCOTT'S property that had been received by the Cambria County Prison with SCOTT following his arrest. This same day, Det. Britton transferred this property to the custody of HSI and it was subsequently transported by your affiant to the HSI Office located in Pittsburgh, PA.

23. The **TARGET DEVICES** described herein are currently stored at Homeland Security Investigations ("HSI"), 3000 Sidney Street, Suite 300, Pittsburgh, PA 15203. Based on training and experience, your Affiant knows that the **TARGET DEVICES** have been stored in a manner in which the contents of the evidence are, to the extent material to this investigation, in substantially the same state as they were when the devices first came into the possession of HSI.

DEFINITIONS

24. The following definitions apply to this Affidavit and Attachment B:

a. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

b. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

c. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals or pubic area of any person.

e. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

f. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" including smart telephones and mobile telephones that are equipped with cameras and data storage capability. *See* 18 U.S.C. § 1030(e)(1).

g. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

h. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

i. "File Transfer Protocol" ("FTP") is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP, built on client-server architecture, uses separate control and data connections between the client and the server.

j. A "hash value" is a unique alpha-numeric identifier for a digital file. A hash value is generated by a mathematical algorithm, based on the file's content. A hash value is a file's "digital fingerprint" or "digital DNA." Two files having identical content will have the same hash value, even if the file names are different. On the other hand, any change to the data in a file, however slight, will change the file's hash value, even if the file name is unchanged. Thus, if two files have the same hash value, they are said to be identical, even if they have different file names.

k. "Internet Protocol address" or "IP address," as used herein, refers to a unique number used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers (ISPs) control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

l. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

m. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

n. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

o. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

p. A "website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language ("HTML") and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol ("HTTP").

CHARACTERISTICS COMMON TO INDIVIDUALS WHO, RECEIVE, POSSESS, AND/OR ACCESS WITH INTENT TO VIEW CHILD PORNOGRAPHY

25. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who receive, possess, and/or access with intent to view child pornography:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals with a sexual interest in children often maintain their child pornography images in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, at the possessor's employment workspace, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

d. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.

e. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses (including e-mail addresses), and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

26. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smart telephones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smart telephone to the computer, using a cable or via wireless connections such as "Wi-Fi" or "Bluetooth." Photos and videos taken on a digital camera or smart telephone may be stored on a removable memory card in the camera or smart telephone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer using telephone, cable, or wireless connection. Mobile devices such as smart telephones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smart telephone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types

– to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices, which plug into a port on the computer – can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smart telephone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Individuals can easily store, carry or conceal media storage devices on their persons. Individuals also often carry Smart telephones and/or mobile telephones.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide e-mail services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smart telephone with access to the Internet. Even in cases where an individual uses online storage, however, law enforcement can find evidence of child pornography on the user's computer, smart telephone or external media in most cases.

g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or

unintentional. Digital information such as the traces of the path of an electronic communication may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information exists indefinitely until overwritten by other data.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

27. As described above and in Attachment B, this application seeks permission to search for records that might be found on evidence specifically described in "Attachment A" that is currently stored at Homeland Security Investigations ("HSI"), 3000 Sidney Street, Suite 300, Pittsburgh, PA 15203. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

28. Your Affiant submits that there is probable cause to believe those records referenced above will be stored on computer(s) or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that forensic examiners can recover computer files or remnants of such files months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using

forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how an individual has used a computer, what the person used it for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation; file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that an individual viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

29. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of

their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which the computer created them, although it is possible for a user to later falsify this information.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search

for "indicia of occupancy" while executing a Search Warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when someone accessed or used the computer or storage media. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or mobile telephone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet

searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records sought, a review team cannot always readily review computer evidence or data in order to pass it along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a person used a computer, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. Your Affiant knows that when an individual uses an electronic device to obtain or access child pornography, the individual's electronic device will generally serve

both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

30. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the later examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

31. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

32. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the **TARGET DEVICES** described in Attachment A to seek the items described in Attachment B.

REQUEST FOR SEALING

33. It is respectfully requested that this Court issue an Order sealing, until further order of this Court, all papers submitted in support of this Application, including the Application, Affidavit, and Search Warrant, and the requisite inventory notice. Sealing is necessary because the items and information to be seized are relevant to an ongoing investigation and premature disclosure of the contents of this Affidavit and related documents may have a negative impact of this continuing investigation and may jeopardize its effectiveness.

Respectfully submitted,

/s/ Jason Adams
JASON ADAMS
Special Agent
Homeland Security Investigations

Sworn and subscribed before me, by telephone
pursuant to Fed. R. Crim. P. 4.1(b)(2)(A),
this 27th day of October 2021.

_____
HONORABLE KEITH A. PESTO
United States Magistrate Judge